(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01794 A2

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/US01/19223

(22) International Filing Date: 14 June 2001 (14.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/605,605 28 June 2000 (28.06.2000) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **ELLISON, Carl** [US/US]; 1818 NW 28th Avenue, Portland, OR 97210 (US). **SUTTON, James, II** [US/US]; 20205 NW Paulina Drive, Portland, OR 97229 (US).

(74) Agent: **MALLIE, Michael, J.**; Blakely Sokoloff Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

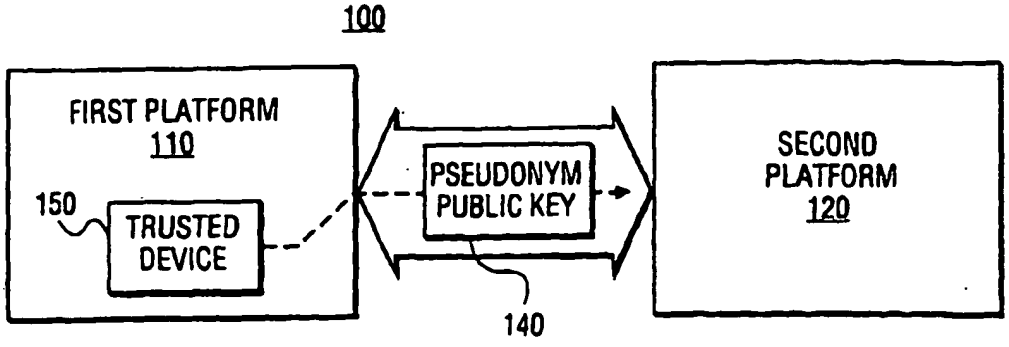
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY



(57) Abstract: In one embodiment, a method for utilizing a pseudonym to protect the identity of a platform and its user is described. The method comprises producing a pseudonym that includes a public pseudonym key. The public pseudonym key is placed in a certificate template. Hash operations are performed on the certificate template to produce a certificate hash value, which is transformed from the platform. Thereafter, a signed result is returned to the platform. The signed result is a digital signature for the transformed certificate hash value. Upon performing an inverse transformation of the signed result, a digital signature of the certificate hash values is recovered. This digital signature may be used for data integrity checks for subsequent communications using the pseudonym.

WO 02/01794 A2

A PLATFORM AND METHOD FOR ESTABLISHING PROVABLE IDENTITIES WHILE MAINTAINING PRIVACY

Field

This invention relates to the field of data security. In particular, the invention relates to a platform and method that protects an identity of the platform through creation and use of pseudonyms.

Background

Advances in technology have opened up many opportunities for applications that go beyond the traditional ways of doing business. Electronic commerce (e-commerce) and business-to-business (B2B) transactions are now becoming popular, reaching the global markets at a fast rate. Unfortunately, while electronic platforms like computers provide users with convenient and efficient methods of doing business, communicating and transacting, they are also vulnerable for unscrupulous attacks. This vulnerability has substantially hindered the willingness of content providers from providing their content in a downloaded, digital format.

Currently, various mechanisms have been proposed to verify the identity of a platform. This is especially useful to determine if the platform features a "trusted" device; namely, the device is configured to prevent digital content from being copied in a non-encrypted format without authorization. One verification scheme involves the use of a unique serial number assigned to a platform for identification of that platform. Another verification scheme, performed either independently from or cooperatively with the previously described verification scheme, involves the use of a permanent key pair. The permanent key pair includes (i) a unique public key that identifies the platform and (ii) a private key that is permanently stored in memory of the trusted device. The private key is confidential and is not provided outside the trusted device. However, these verification schemes pose a number of disadvantages.

For example, each of these verification schemes is still subject to data aggregation attacks. "Data aggregation" involves the collection and analysis of data transmitted from a platform over a period of time. Thus, the use of platform serial numbers and permanent keys for identification purposes has recently lead to consumer privacy concerns. Also, for both verification mechanisms, a user cannot easily and reliably control access to and use of the platform identity on a per-use basis.